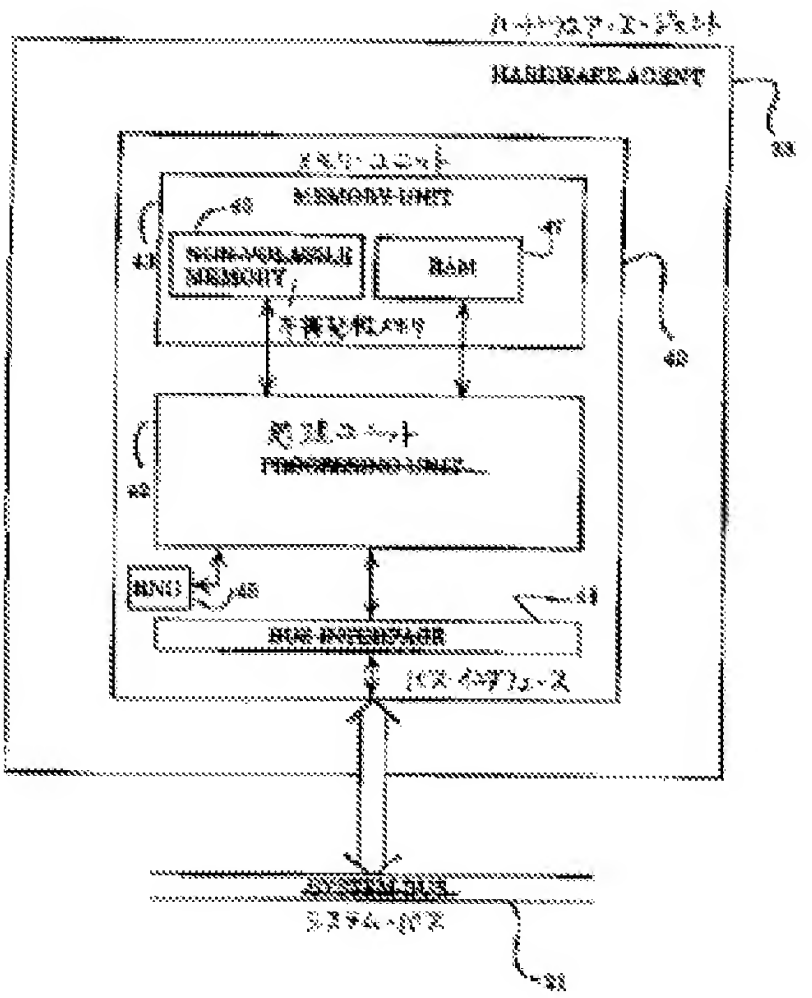
DEVICE AND METHOD FOR SECURITY COMMUNICATION

Patent number: JP9200194
Publication date: 1997-07-31
Inventor: DEREEKU ERU DEIBISU
Applicant: INTEL CORP
Classification:
- international: ***H04L9/08; G09C1/00; H04L9/10;*** **H04L9/08; G09C1/00; H04L9/10;** (IPC1-7): H04L9/10; G09C1/00; H04L9/08
- european:
Application number: JP19950353850 19951229
Priority number(s): JP19950353850 19951229

Abstract of **JP9200194**

PROBLEM TO BE SOLVED: To reduce the danger of accidental disclosure of a public key/a private key in pairs against an illegal recipient by providing a storage means storing the keys in pairs and a digital certificate and a storage means storing processed information. SOLUTION: A hardware agent 23 is made up of a single integrated circuit of a form of an enclosed die 40 and the die 40 is made up of a memory unit 43, and a picture unit 42 connecting to a bus interface 44 and a anumeral generator 45. The bus interface allows communication from the hardware agent 23 to other device. Then the memory unit 43 includes a nonvolatile memory element 46 storing a public key/a private key in pairs and at least one digital certificate Moreover, the memory unit 43 includes a random access memory(RAM) 47 to store some results from the processing unit 42 and a corresponding algorithm.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－200194

(43)公開日　平成９年(1997)７月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/10			Ｈ０４Ｌ	9/00	６２１Ａ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｚ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ｚ

審査請求　未請求　請求項の数８　ＦＤ　（全 15 頁）

(21)出願番号　特願平7－353850

(22)出願日　平成７年(1995)12月29日

(71)出願人　591003943
インテル・コーポレーション
アメリカ合衆国　95052　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・2200

(72)発明者　デレーク・エル・デイビス
アメリカ合衆国　85044　アリゾナ州・フィーニクス・イースト　アシャースト　ドライブ・4129

(74)代理人　弁理士　山川　政樹

(54)【発明の名称】　安全保護の行われた通信を行うための装置および方法

(57)【要約】

【課題】　半導体デバイスと他の装置の間の安全保護された通信を確保する。

【解決手段】　ディジタル証明書と組み合わせて暗号化とその解読キーを記憶する。半導体デバイスは暗号化とその解読キーと少なくとも１つのディジタル証明書を記憶するための不揮発性メモリと、他の装置および恐らくは暗号化とその解読アルゴリズムから半導体デバイスに入力された情報を一時的に記憶する内部メモリと、ハードウェア・エージェントに対して暗号化とその解読キーを完全に内部的に生成する乱数発生器とを備えている。

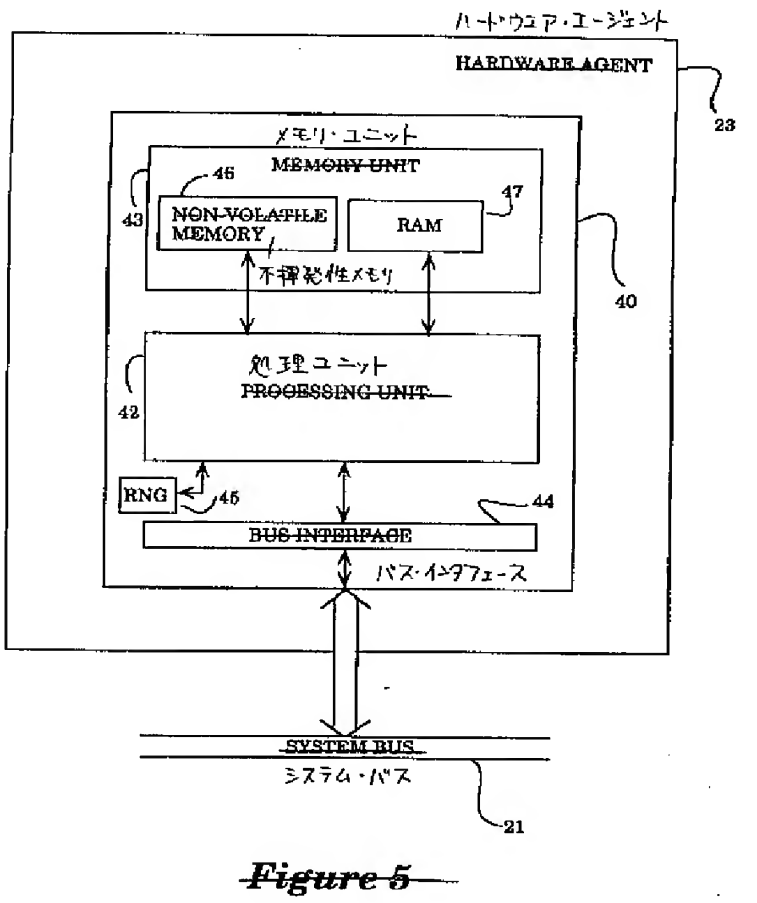


Figure 5

【特許請求の範囲】
【請求項１】　半導体デバイスにおいて、
その半導体デバイス内の情報を処理する処理手段と、
前記処理手段に結合され、独特に指定されたキー・ペアと少なくとも１つのディジタル証明書とを記憶する第１記憶手段と、
前記処理手段に結合され、前記処理手段によって処理された前記情報を少なくとも記憶する第２記憶手段と、
前記処理手段に結合され、前記半導体デバイスと第２の半導体デバイスの間の通信を可能とするインタフェース手段とを備えていることを特徴とする前記半導体デバイス。
【請求項２】　情報の符号化および復号化を行う半導体デバイスにおいて、
独特に指定されたキー・ペアと少なくとも１つのディジタル証明書とを記憶する不揮発性メモリと、
前記情報を記憶するランダム・アクセス・メモリと、
前記不揮発性メモリと前記ランダム・アクセス・メモリとに結合され、前記情報を少なくとも内部的に処理する処理ユニットと、
前記処理ユニットに結合され、前記半導体デバイスが少なくとも第２の半導体デバイスと通信を行うのを可能とするインタフェースとを備えていることを特徴とする前記半導体デバイス。
【請求項３】　前記の独特に指定されたキー・ペアを生成するための乱数発生器をさらに含んでおり、その乱数発生器が前記処理ユニットに結合されている請求項２に記載の半導体デバイス。
【請求項４】　少なくとも１つの暗号化／解読プログラムを記憶するメモリ手段と、
前記暗号化とその解読プログラムを実行するホスト処理手段と、
そのホスト処理手段と前記メモリ手段とを結合するバス手段と、
そのバス手段に結合され、入力情報を内部的に解読し、出力情報を暗号化するエージェント手段とを備えており、
そのエージェント手段が前記入力および出力情報を処理する処理手段と、
前記処理手段に結合され、前記入力信号を解読し、前記出力信号を暗号化するために使用される独特に指定されたキー・ペアと少なくとも１つのディジタル証明書とを記憶する第１記憶手段と、
少なくとも前記入力および出力情報を一時的に記憶する第２記憶手段と、
前記処理手段に結合され、システムと遠隔システムの間の安全保護された通信を可能とするインタフェース手段とを含んでいることを特徴とするシステム。
【請求項５】　少なくとも１つの暗号化とその解読プログラムを記憶するメモリ要素と、
前記暗号化とその解読プログラムを実行するためのホスト・プロセッサと、
そのホスト・プロセッサと前記メモリ要素を結合するバスと、
そのバスに結合され、遠隔装置からの入力情報を内部的に解読し、出力情報をその遠隔装置に伝送するために暗号化するハードウェア・エージェントを備えており、
そのハードウェア・エージェントがハードウェア・エージェント内の前記入力および出力情報を処理するプロセッサと、
前記プロセッサに結合され、両方とも前記入力情報の解読、および前記出力情報の暗号化に使用される独特に指定されたキー・ペアと装置証明書を記憶する不揮発性記憶要素と、
前記入力および出力情報を一時的に記憶する揮発性記憶要素と、
前記の独特に指定されたキー・ペアを生成する乱数発生器と、
前記プロセッサに結合され、前記ハードウェア・エージェントと前記遠隔装置との間の安全保護された通信を可能とするインタフェースとを含んでいることを特徴とするシステム。
【請求項６】　他の遠隔装置との安全保護された通信を確実に行うために利用されるハードウェア・エージェントを作成する方法において、
前記ハードウェア・エージェントが証明システムと電気的接続を確立するように前記ハードウェア・エージェントを前記証明システムに置くステップと、
前記ハードウェア・エージェントにまず電力を供給し、
前記ハードウェア・エージェント内の乱数発生器が装置固有のキー・ペアを生成する構成シーケンスを開始するステップと、
前記の装置固有のキー・ペアが独特であることを検査するステップと、
前記の装置固有のキー・ペアを前記ハードウェア・エージェント内の不揮発性記憶要素に記憶するステップとを備えていることを特徴とする前記方法。
【請求項７】　独特の装置証明書を作成するステップと、
その装置証明書を前記ハードウェア・エージェントに入力するステップと、
前記装置証明書を前記ハードウェア・エージェントの前記不揮発性記憶要素に記憶するステップとをさらに含んでいる請求項６に記載の方法。
【請求項８】　独特の第２レベル証明書を作成するステップと、
その第２レベル証明書を前記ハードウェア・エージェントに入力するステップと、
前記第２レベル証明書を前記ハードウェア・エージェントの前記不揮発性記憶要素に記憶する手段とをさらに含

んでいる請求項７に記載の方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データ・セキュリティのための装置および方法に関する。詳細にいえば、本発明は製造時および／または製造後に暗号化とその解読キーを格納する半導体デバイスに関し、半導体デバイスを組み込んだシステムとそのシステムと遠隔通信を行う装置との間での安全保護された通信を確保するものである。
【０００２】
【従来の技術】今日の社会においては、正当な受信者にとっては明確で曖昧なところがないが、不法な受信者には理解できない態様で、ディジタル情報をある場所から他の場所へ伝送することがますます望まれるようになっている。したがって、このような情報は通常、ある種の所定の暗号化アルゴリズムを実行するソフトウェア・アプリケーションによって暗号化し、暗号化された形態で正当な受信者へ伝送される。正当な受信者は伝送されてきた情報を解読して使用する。この暗号化とその解読伝送プロセスは一般に、政府で使用されており、また、機密情報を伝送する場合に、民間でも使用されている。
【０００３】情報の暗号化とその解読が図１に示す対称キー暗号作成法によって達成されることがしばしばある。対称キー暗号作成法においては、同一のキー１（すなわち、一般に「対称キー」と呼ばれるデータ・ストリング）を正当な送信者２と正当な受信者３の両方が使用して、送信者２と受信者３の間で伝送されるメッセージ４（すなわち、情報）の暗号化および解読を行っている。このような暗号化および解読はＲＡＳ、ＤＥＳなどの従来からある周知のアルゴリズムによって行われ、在来のネットワーク、電話回線などの公共施設を通じて、暗号化された形態で伝送が行われる。
【０００４】対称キー暗号作成法は演算自体の面で単純なものであるが、複雑なキーの管理を必要とする。基本的に、各送信者は正当な各受信者との通信に異なる対称キーを必要とし、これにより、多数の従業員のいる企業で使用するのが、不可能とはいえないにしても困難となる。たとえば、１０００の正当なエンティティ（たとえば、従業員）のある企業においては、各正当なエンティティが企業内の他のエンティティと通信できる場合、最大限４９９，５００（１０００×９９／２）個のキーを管理する必要がある。さらに、対称キーを正当な送信者２から正当な受信者３へ伝送する確実で、便利な方法がないため、対称キー暗号作成法をネットワークや大域環境で実施するのは困難である。
【０００５】他の暗号化とその解読方法は２つの別々のキー（「キー・ペア」と呼ぶ）を使用するものであり、図２に示すように、キー・ペアのうち第１のキー（「公開キー」）１０は正当な送信者１３からのメッセージ１２の暗号化に使用され、キー・ペアのうち第２のキー（「私用キー」）１１は正当な受信者１４によるメッセージ１２の解読に使用される。この方法は一般に「非対称」（または、公開）キー暗号作成法と呼ばれている。非対称キー暗号作成法の利点の１つは、対称キー暗号作成法に関連するわずらわしいキー管理の問題を軽減することである。上記の例について説明を続けると、非対称暗号化作成法に必要なキー・ペアの数は１０００、すなわち正当なエンティティの総数に等しい。しかしながら、このような通信システムにおいては、不法なエンティティ（たとえば、産業スパイ）が業務の流れを混乱させたり、機密情報を入手することを目的として、偽のメッセージを他の正当なエンティティに送ることによって、正当なエンティティ（たとえば、従業員、合弁事業会社）を装うと試みることがある。それ故、付加的なプロトコルを非対称キー・システムに使用して、メッセージと発信者の認証を行うのが普通である。
【０００６】発信者の認証（すなわち、公開キーの発信者が実際に公開キーの真の所有者であることを確認する）は、通信をそれまで未知の当事者の間で初めて確立するときに問題となる。この問題は一般に、図３に示すように、送信メッセージ１２内にディジタル証明書１５を組み込むことによって回避される。ディジタル証明書１５は相互に信任した機関１６（たとえば、銀行、政府機関、業者団体など）によって発行されるもので、他人の公開キー１０を使用しようという不正を試みても、判読できないメッセージがもたらされるだけとなる。このような相互信任機関１６は関与する当事者によって異なっている。たとえば、同一の企業に雇用されている２人の人間はその企業の社内セキュリティ・オフィスが発行した証明書を両者ともに信用することとなる。２つの独立した企業の従業員は、しかしながら、それぞれの会社のセキュリティ・オフィスの証明書だけでなく、たとえば、このような企業エンティティの証明を行う業界団体の証明書も必要とすることになろう。このディジタル証明機関１６による方法は公開キー１０をエンティティ（たとえば、従業員）に「拘束」するものである。
【０００７】ここ数年間に、「キー」情報が無許可の人間に取得されることを防止する多くの方式が出てきている。このような方式の１つは、特に盗難が容易なポータブル・コンピュータ用に機械的なセキュリティ機構を用いるものである。たとえば、いくつかの会社はラップトップのケースを許可なく開いた場合にキー資料を消去する不法行為検出機構を使用したラップトップを発表している。しかしながら、機械的なセキュリティ装置には、いくつかの関連した欠点がある。
【０００８】機械的セキュリティ装置に関連した主な欠点は、これらをリバース・エンジニアリングによってごまかせることがあることである。他の欠点は、機械的なセキュリティ機構を設計し、製造することは費用がかか

るということである。また他の欠点はキー情報が偶発的に消去される可能性があることである。
【０００９】結果として、多くの会社は暗号化とその解読プロトコルを使用したソフトウェア・アプリケーションだけに依存することとなっている。しかしながら、技術が迅速に発展するにともない、これらの暗号化とその解読ソフトウェア・アプリケーションは、情報の暗号化および解読速度が命令の実行速度に相関しているため、通信システムの伝送速度に不必要な制限を課すものとなる。
【００１０】特定のハードウェアを顧客のシステムに用いて、このようなキーを開示から保護するというこの方式は、急速に成長している「コンテンツ流通」、すなわち情報の電子的な流通の分野でも使用されている。周知のコンテンツ流通システムの中には、（ｉ）モデムその他の電子的手段によってソフトウェアを販売するもの、（ｉｉ）コンパクト・ディスク（「ＣＤ」）によって配布された情報の一部を販売するものなどがある。このような電子的な販売は関連する特定のデータを「復号」するための解読キーに依存している。たとえば、顧客は暗号化されたデータの多くのファイルを収めているＣＤに自由にアクセスできるが、特定のファイルを購入するには、そのファイルに対応した「解読キー」を購入しなければならない。しかしながら、キーを保護するために特定のハードウェアを使用する際の主な問題は、このようなハードウェアが無許可の使用の可能性をなくするために、情報の供給業者による完全な管理および統制を必要とすることである。
【００１１】
【発明が解決しようとする課題】上記したところに基づき、少なくとも処理ユニットと、公開／私用キー・ペアを製造時に、また半導体デバイスを組み込んだシステムと他の遠隔システムの間に安全保護がより確実に行われる通信をもたらすための少なくとも１つのディジタル証明書を製造時および／またはそれ以降に記憶するための不揮発性メモリ要素とを有する半導体デバイスを開発することが望ましい。したがって、本発明の目的は、不法な受信者に対する公開／私用キー・ペアの偶発的開示の危険性をかなり減じる半導体デバイスを提供することである。
【００１２】本発明の他の目的は、独特の公開／私用キー・ペアを内部で生成できる半導体デバイスを提供することである。
【００１３】本発明のさらに他の目的は、安全保護のなされていない半導体デバイス外での私用キーの使用を防止するために私用キーを記憶する半導体デバイスを提供することである。
【００１４】本発明のさらにまた他の目的は、リバース・エンジニアリングによるキー・ペアの検出を実質的に防止するために集積回路内での公開／私用キー・ペアの記憶および使用に対して安全保護を施す半導体デバイスを提供することである。
【００１５】本発明の他の目的は、デバイスを遠隔（電子的に）認証し、個々のユニットを識別するための独特のディジタル証明書を記憶する半導体デバイスを提供することである。
【００１６】本発明の他の目的は、独特性および自己認証という機能により、遠隔エンティティ（コンテンツ流通業者など）に代わって補償された職務を遂行できる装置を提供することである。
【００１７】本発明の他の目的は、データ通信および記憶のための費用効果の高い装置を提供することである。
【００１８】
【課題を解決するための手段】半導体デバイスは、識別のための操作を行う処理ユニットと、独特の公開／私用キー・ペア、ならびにキー・ペアの真性性を確認する少なくとも１つのディジタル証明書を記憶するための少なくとも１つの不揮発性メモリと、暗号作成アルゴリズムを記憶するためのメモリと、一時データを記憶するための揮発性ランダム・アクセス・メモリとを備えたハードウェア・エージェントである。ハードウェア・エージェントはさらに、他の装置との情報（暗号化または解読された）の送受信のためのインタフェースを含んでいる。
【００１９】本発明の目的、特徴および利点は本発明に関する以下の詳細な説明から明らかとなろう。
【００２０】
【発明の実施の形態】本発明は公開／私用キー・ペアおよび少なくとも１つのディジタル証明書をハードウェア・エージェント自体内に安全に記憶し、かつ使用することを対象としたハードウェア・エージェントおよびこれに関連した操作方法に関する。このディジタル証明書は装置の正当性を表す装置の製造業者が与えるディジタル証明書である「装置証明書」と、信任された第三者によるディジタル証明書である「第２レベル証明書」とを含んでいても、あるいは両方の証明書を集めたものを含んでいてもよい。以下の説明において、本発明を完全に理解させるためハードウェア・エージェントのいくつかの構成要素などのさまざまな細部が記載されている。しかしながら、当分野の技術者には、これらの細部が本発明の実施に必要ではないことが明らかであろう。場合によっては、本発明を不要に曖昧なものとしないために、周知の回路、要素などの詳細を記載しない。
【００２１】図４を参照すると、本発明を利用するコンピュータ・システム２０が示されている。コンピュータ・システム２０は少なくとも１つのホスト・プロセッサ２２とハードウェア・エージェント２３を含む複数のバス・エージェントの間で情報を通信することを可能とするシステム・バス２１を含んでいる。Ｉｎｔｅｌ（登録商標）アーキテクチャのプロセッサであることが好ましいが、これに限定されるものではないホスト・プロセッ

サ２２はプロセッサ・バス・インタフェース２４を介してシステム・バス２１に結合されている。本実施形態にはホスト・プロセッサ２２だけしか示されていないが、複数個のプロセッサをコンピュータ・システム２０内に用いることも考えられている。

【００２２】図４にさらに示すように、システム・バス２１はメモリ・サブシステム２５および入出力（Ｉ／Ｏ）サブシステム２６へアクセスできるようにする。メモリ・サブシステム２５はシステム・バス２１に結合されたメモリ・コントローラ２７を含んでおり、ダイナミック・ランダム・アクセス・メモリ（「ＤＲＡＭ」）、読取り専用メモリ（「ＲＯＭ」）、ビデオ・ランダム・アクセス・メモリ（「ＶＲＡＭ」）などの少なくとも１つのメモリ装置に対するアクセスを制御するインタフェースをもたらす。メモリ装置２８はホスト・プロセッサ２２用の情報および命令を記憶している。

【００２３】Ｉ／Ｏサブシステム２６は、システム・バス２１および従来のＩ／Ｏバス３０に結合されたＩ／Ｏコントローラ２９を含んでいる。Ｉ／Ｏコントローラ２９はＩ／Ｏバス３０とシステム・バス２１の間のインタフェースであり、システム・バス２１またはＩ／Ｏバス３０上の装置が情報を交換するのを可能とする通信経路（すなわち、ゲートウェイ）をもたらす。Ｉ／Ｏバス３０は、画像を表示するための表示装置３１（たとえば、陰極線管、液晶表示装置など）、ホスト・プロセッサ２２に対して情報およびコマンドの選択を伝えるための英数字入力装置３２（たとえば、英数字キーボードなど）、カーソルの運動を制御するためのカーソル制御装置３３（たとえば、マウス、トラックボールなど）、情報および命令を記憶するための大容量記憶装置３４（たとえば、磁気テープ、ハード・ディスク装置、フロッピー・ディスク装置など）、コンピュータ・システム２０と他の装置の間で情報を送受信するための情報送受信機３５（ファックス装置、モデム、スキャナなど）、および情報の有形な視覚的表示をもたらすハード・コピー装置３６（たとえば、プロッタ、プリンタなど）を含んでいるが、これらに限定されるものではないコンピュータ・システム２０の少なくとも１つの周辺装置との間で情報を通信する。図４に示したコンピュータ・システムがこれらの構成要素のあるものまたはすべて、あるいは図示のものとは異なる構成要素を用いることができると考えることができる。

【００２４】図５に示すような本発明の実施形態を参照すると、ハードウェア・エージェント２３はホスト・プロセッサ２２との通信経路を確立するためにシステム・バス２１に結合されている。ハードウェア・エージェント２３は半導体デバイス・パッケージ内に、好ましくは気密に、封入されたダイ４０（たとえば、マイクロコントローラ）の形態の単一の集積回路からなっており、ダイ４０を損傷および有害な汚染物から保護している。ダイ４０はメモリ・ユニット４３、バス・インタフェース４４および数値発生器４５に結合された処理ユニット４２からなっている。バス・インタフェース４４はハードウェア・エージェント２３から他の装置（たとえば、ホスト・プロセッサ２２）への通信を可能とする。処理ユニット４２はダイ４０内の安全保護環境内で計算を行って、許可を受けた受信者との有効な接続を確認する。このような計算には、ある種のアルゴリズムおよびプロトコルの実行、装置固有の公開／私用キー・ペアなどを発生するための回路（たとえば、本質的に乱数であることが好ましい数値発生器４５）の活動化などがある。処理ユニット４２は、私用キーを取得するためにコンピュータ・システムを混乱させる一般的な方法であるウィルスの攻撃による私用キーのアクセスを防止するため、ダイ４０内に配置されている。

【００２５】メモリ・ユニット４３は公開／私用キー・ペアおよび少なくとも１つのディジタル証明書を記憶する不揮発性メモリ要素４６を含んでいる。供給電力が停止したときに内容を保持するので、不揮発性メモリ４６が使用される。メモリ・ユニット４３は処理ユニット４２および該当するアルゴリズムからのある種の結果を記憶するためにランダム・アクセス・メモリ（「ＲＡＭ」）４７をさらに含んでいる。

【００２６】ハードウェア・エージェント２３はセキュリティを高めるためシステム・バス２１の周辺装置として実現されているが、ハードウェア・エージェント２３をＰＣプラットフォーム・レベルで、たとえば、ハード・ディスクに対して入出力される情報を自動的に解読および／または暗号化するためのディスク・コントローラまたはＰＣＭＣＩＡカードなどのいくつかの他の態様で実施することも考えられる。他の代替実施形態はハードウェア・エージェント２３を以下で説明するようなホスト・プロセッサ２２を含むマルチチップ・モジュールの構成要素の１つとすることである。さらに、ハードウェア・エージェント２３をＰＣプラットフォームに関連して説明するが、このようなハードウェア・エージェント２３をファックス装置、プリンタなどの任意の入出力（「Ｉ／Ｏ」）周辺装置内で、あるいはコンピュータとＩ／Ｏ周辺装置の間の通信経路上で実施することも考えられる。

【００２７】図６を参照すると、本発明を製造するための操作の流れ図が示されている。まず、ステップ１００において、ハードウェア・エージェントのダイが従来の周知の半導体製造技法にしたがって製造される。次に、ダイを半導体パッケージ内に封入して、ハードウェア・エージェント自体を形成する（ステップ１０５）。ハードウェア・エージェントを、ハードウェア・エージェントと証明システムへの電気的接続を確立する証明システムに入れる（ステップ１１０）。証明システムは基本的に、ハードウェア・エージェントの証明のための電気信

号を発生し、受け取るための、プリント回路ボードに結合された担持体である。証明システムは独特のキーの生成を保証するために以前に生成された公開キーを記憶するための装置（たとえば、データベース）を含んでいる。次いで、証明システムはハードウェア・エージェントに電力を供給して、構成手順を開始する。この手順の間、乱数発生器は装置固有の公開／私用キー・ペアをハードウェア・エージェント内部で生成する（ステップ１１５）。

【００２８】公開／私用キー・ペアの公開キーは証明システムに対して出力され（ステップ１２０）、以前に製造されたハードウェア・エージェントからの以前に生成された公開キーの記憶装置と比較される（ステップ１２５）。公開キーが以前に生成された公開キーと同一であるというきわめて起こりにくい状況においては（ステップ１３０）、ハードウェア・エージェントに他のこのような公開／私用キー・ペアを生成するようにという通知が証明システムによって行われ（ステップ１３５）、ステップ１２０のプロセスを継続する。このプロセスは各公開／私用キー・ペアが独特のものであることを確実とするものである。以前に生成された公開キーの記憶装置はこの新しい独特の公開キーによって更新される（ステップ１４０）。その後、ステップ１４５において、証明システムは製造業者の秘密の私用キーを用いて公開キーに「ディジタル署名」する（一般的な言い方をすれば、製造業者の私用キーを用いて公開キーを暗号化する）ことによって、独特の装置証明書を作成する。この証明書はハードウェア・エージェントに入力され（ステップ１５０）、ハードウェア・エージェントは独特の公開／私用キー・ペアおよび装置証明書を不揮発性メモリに永続的にプログラムする（ステップ１５５）。この時点で、装置は物理的に独特のものとなり、その真性性をもたらすことができる。

【００２９】図７を参照すると、ハードウェア・エージェントの遠隔検証の流れ図が示されている。ステップ２００において、ハードウェア・エージェントが組み込まれたシステム（「ハードウェア・エージェント・システム」）と遠隔システムとの間に通信リンクが確立される。遠隔システムとは、たとえば、他のハードウェア・エージェントが組み込まれていたり、あるいはハードウェア・エージェントと通信するソフトウェアを実行するシステムである。ハードウェア・エージェントはその独特の装置証明書を遠隔システムに対して出力する（ステップ２０５）。製造業者の公開キーが公開されており、一般に入手できるものであるため、遠隔システムは装置証明書を解読して、ハードウェア・エージェントの公開キーを取得する（ステップ２１０）。

【００３０】その後、ステップ２１５において、遠隔システムはランダムな呼掛け（すなわち、テスト用のデータ・シーケンス）を生成し、これをハードウェア・エージェント・システムに伝送する（ステップ２２０）。ステップ２２５において、ハードウェア・エージェントは応答を生成し（すなわち、ハードウェア・エージェントの私用キーを用いて呼掛けを暗号化し）、これを遠隔システムへ伝送する（ステップ２３０）。次いで、遠隔システムはハードウェア・エージェントから伝送された装置証明書から予め決定したハードウェア・エージェントの公開キーを使用して応答を解読する（ステップ２３５）。ステップ２４０において、遠隔システムは元の呼掛けを解読した応答と比較し、同一であれば、システムと遠隔システムの間の通信は安全であり、維持される（ステップ２４５）。それ以外の場合、通信は打ち切られる（ステップ２５０）。この時点で、遠隔システムには、特定の製造業者が製造した特定の装置（既知の特性の）と直接更新していることが保証される。ここで、遠隔システムはハードウェア・エージェントに遠隔システムに代わってターゲット・システム内で特定の機能を実行するよう指示することができる。これらの機能の整合性および関連するデータの機密性が保証される。このような機能にはコンテンツ流通キーの受信および使用、ならびに会計情報の維持などがある。

【００３１】他の情報提供装置とともにコンテンツの流通が出現したことにともない、ハードウェア・エージェントが偽物ではないことの付加的な確認を与えるのが必要となる可能性がある。これはハードウェア・エージェントを含む半導体デバイスを、たとえば政府機関、銀行、業界団体などの信頼できる第三者エンティティに送ることによって達成できる。上述したのと同じ態様で、第三者エンティティの独特の第三者ディジタル証明書（「第２レベル証明書」）がハードウェア・エージェントに入力される。その後、ハードウェア・エージェントは第２レベル証明書を公開／使用キー・ペアおよび恐らくは装置証明書とともに不揮発性メモリに永続的にプログラムする。結果として、ハードウェア・エージェントは装置証明書および第２レベル証明書の両方によって確認され、ハードウェア・エージェントの妥当性が保証され、ハードウェア・エージェントの不正な製造が防止され、第三者エンティティとハードウェア・エージェントの製造業者による、行われるとは思われない共謀が防がれる。

【００３２】図８を参照すると、第２レベル証明書を使用した認証を含むハードウェア・エージェントの遠隔検証の流れ図が示されている。ステップ３００において、通信リンクがハードウェア・エージェント・システムと遠隔システムの間に確立される。ハードウェア・エージェントはその独特の装置証明書と第２レベル証明書を遠隔システムに対して出力する（ステップ３０５）。次に、遠隔システムは製造業者が公表している公開キーを使用して装置証明書を解読し、ハードウェア・エージェントの公開キーを取得する（ステップ３１０）。同様

に、遠隔システムは第三者の完全に公表されている公開キーを使用して、ハードウェア・エージェントに記憶されているハードウェア・エージェントの公開キーを取得する（ステップ３１５）。

【００３３】その後、ハードウェア・エージェントの２つのバージョンの公開キーが比較され（ステップ３２０）、２つのバージョンが同一でない場合には、通信が打ち切られる（ステップ３２５）。しかしながら、２つのバージョンが同一の場合には、遠隔システムはランダムな呼掛けを生成し、これをハードウェア・エージェントに伝送する（ステップ３３０）。ハードウェア・エージェントは応答、すなわちハードウェア・エージェントの私用キーを用いて暗号化した呼掛けを生成し（ステップ３３５）、これを遠隔システムに伝送する（ステップ３４０）。遠隔システムは次いで、ハードウェア・エージェントから予め伝送されているハードウェア・エージェントの公開キーを用いて応答を解読する（ステップ３４５）。ステップ３５０におけるように、遠隔システムは元の呼掛けを解読した応答と比較し、同一であれば、システムと遠隔システムの間の通信は安全であり、維持される（ステップ３５５）。それ以外の場合には、通信が打ち切られる（ステップ３６０）。

【００３４】本発明を多くの異なる方法で、かつ多くの異なる構成を使用して設計することができる。本発明をさまざまな実施形態によって説明したが、本発明の精神および範囲を逸脱することなく、他の実施形態が当分野の技術者には思い浮かべられるであろう。したがって、本発明は特許請求の範囲だけによって判断されるべきである。

【図面の簡単な説明】

【図１】従来の対称キー暗号化および解読プロセスを説明するブロック図である。

【図２】従来の非対称キー暗号化および解読プロセスを説明するブロック図である。

【図３】信任された機関によるディジタル証明プロセスを説明するブロック図である。

【図４】本発明の実施形態を組み込んだコンピュータ・システムのブロック図である。

【図５】本発明の実施形態のブロック図である。

【図６】キー・ペアおよびディジタル証明書を半導体デバイスで実施する方法を説明する流れ図である。

【図７】ハードウェア・エージェントの作動を説明する流れ図である。

【図８】第２レベルの証明を使用したハードウェア・エージェントの遠隔検証を説明する流れ図である。

【符号の説明】

２０　コンピュータ・システム
２１　システム・バス
２２　ホスト・プロセッサ
２３　ハードウェア・エージェント
２５　メモリ・サブシステム
２６　Ｉ／Ｏサブシステム
２７　メモリ・コントローラ
２８　メモリ装置
４０　ダイ
４１　半導体デバイス・パッケージ
４２　処理ユニット
４３　メモリ・ユニット
４４　バス・インタフェース
４５　数値発生器
４６　不揮発性メモリ要素
４７　ランダム・アクセス・メモリ

【図１】

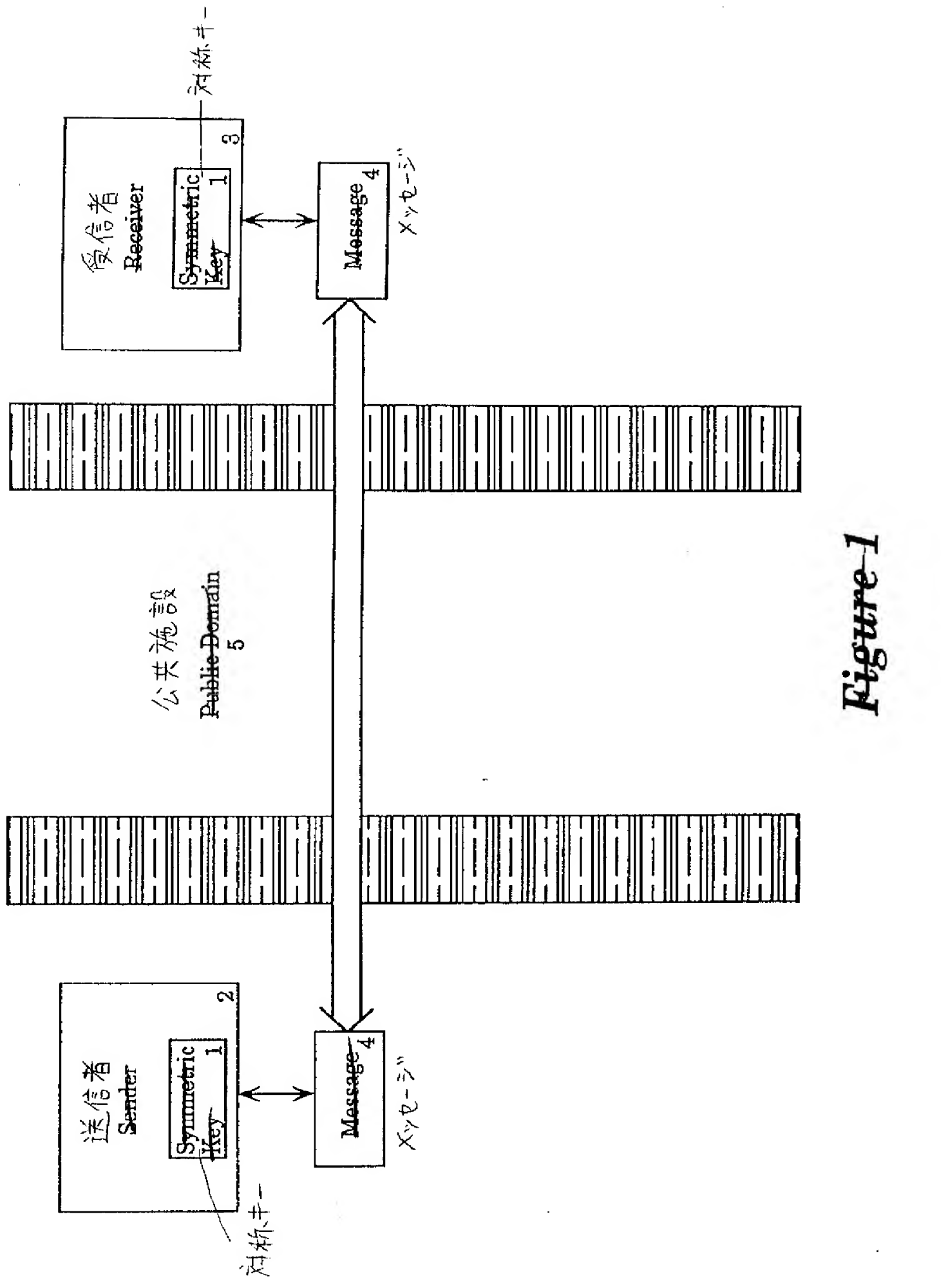

受信者
Receiver
Symmetric Key 1
3
対称キー
Message 4
メッセージ
公共施設
Public Domain
5
送信者
Sender
Symmetric Key 1
2
対称キー
Message 4
メッセージ

Figure 1

【図２】

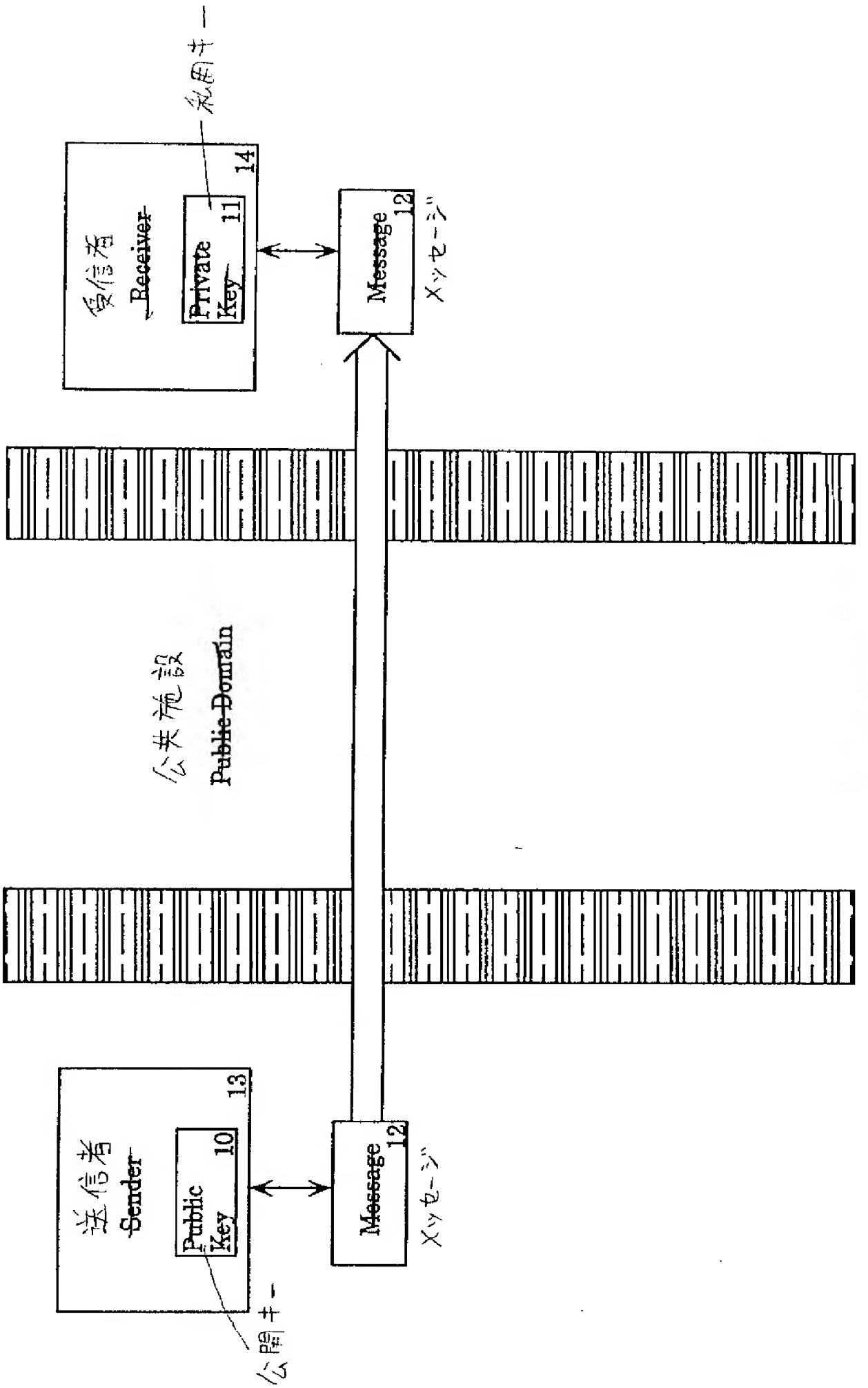

受信者
Receiver
Private Key 11
14
秘密キー
Message 12
メッセージ
公共施設
Public Domain
送信者
Sender
Public Key 10
13
公開キー
Message 12
メッセージ

Figure 2

【図3】

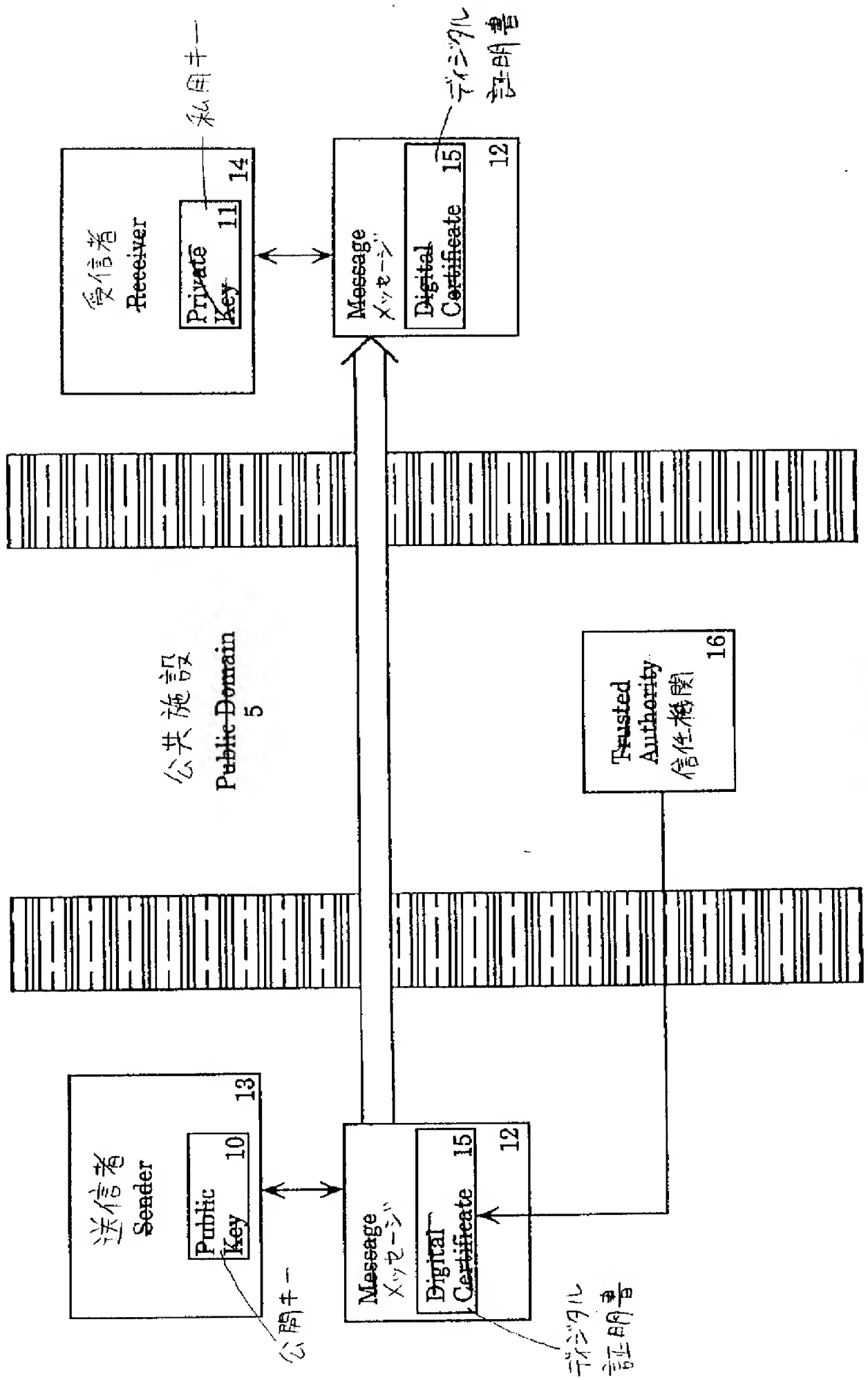

受信者
Receiver
Private Key
11
14
私用キー
Message
メッセージ
Digital Certificate
15
12
ディジタル証明書
公共施設
Public Domain
5
Trusted Authority
信任機関
16
送信者
Sender
Public Key
10
13
公開キー
Message
メッセージ
Digital Certificate
15
12
ディジタル証明書

Figure 3

【図4】

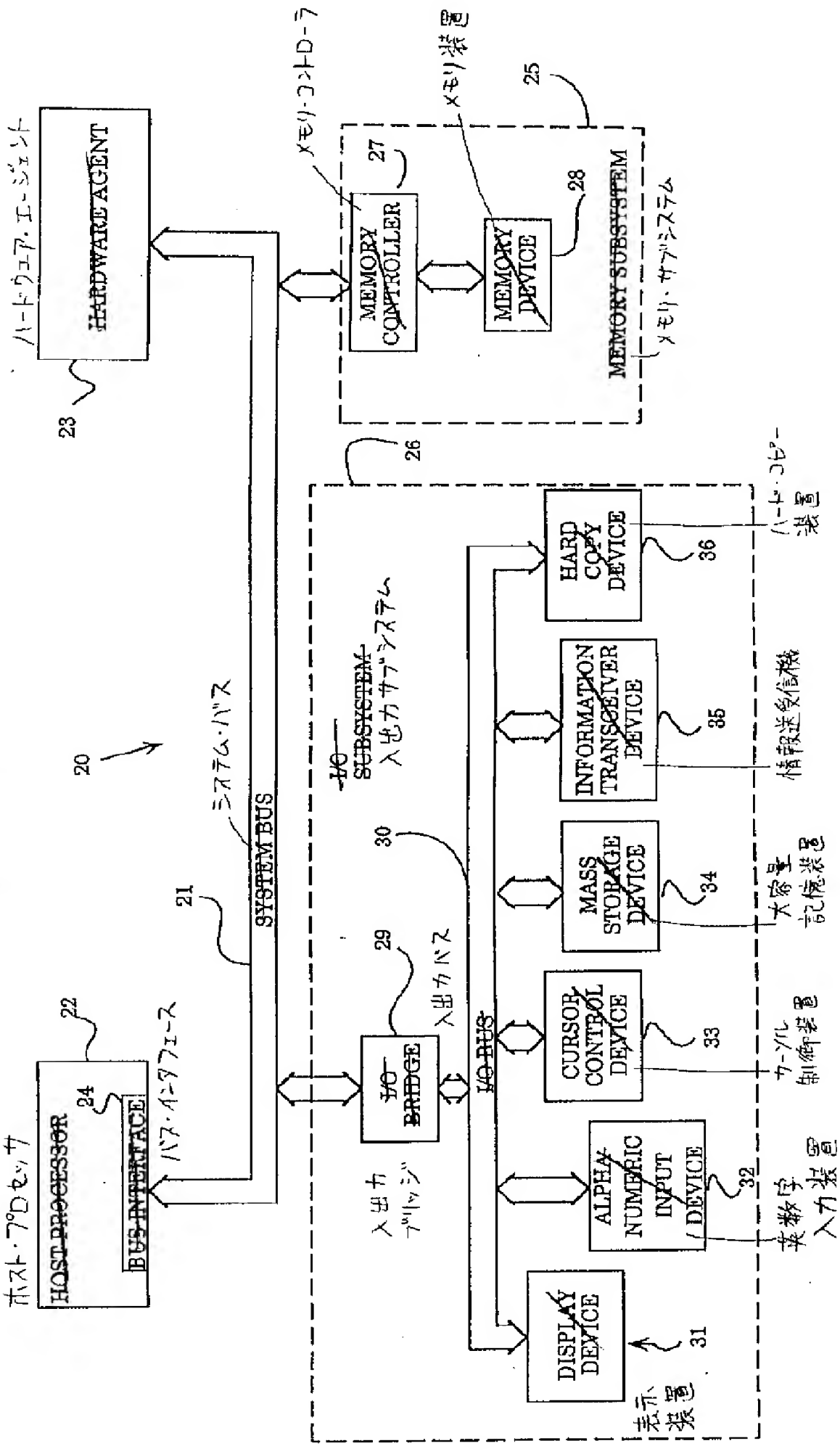

ハードウェア・エージェント
HARDWARE AGENT
23
メモリ・コントローラ
メモリ装置
25
27
28
MEMORY CONTROLLER
MEMORY DEVICE
メモリ・サブシステム
MEMORY SUBSYSTEM
26
ハード・コピー装置
HARD COPY DEVICE
36
20
ホスト・プロセッサ
HOST PROCESSOR
22
24
BUS INTERFACE
バス・インタフェース
21
システム・バス
SYSTEM BUS
I/O SUBSYSTEM
入出力サブシステム
30
29
I/O BRIDGE
入出力ブリッジ
入出力バス
I/O BUS
INFORMATION TRANSCEIVER DEVICE
35
情報送受信機
MASS STORAGE DEVICE
34
大容量記憶装置
CURSOR CONTROL DEVICE
33
カーソル制御装置
ALPHA-NUMERIC INPUT DEVICE
32
英数字入力装置
DISPLAY DEVICE
31
表示装置

Figure 4

【図５】

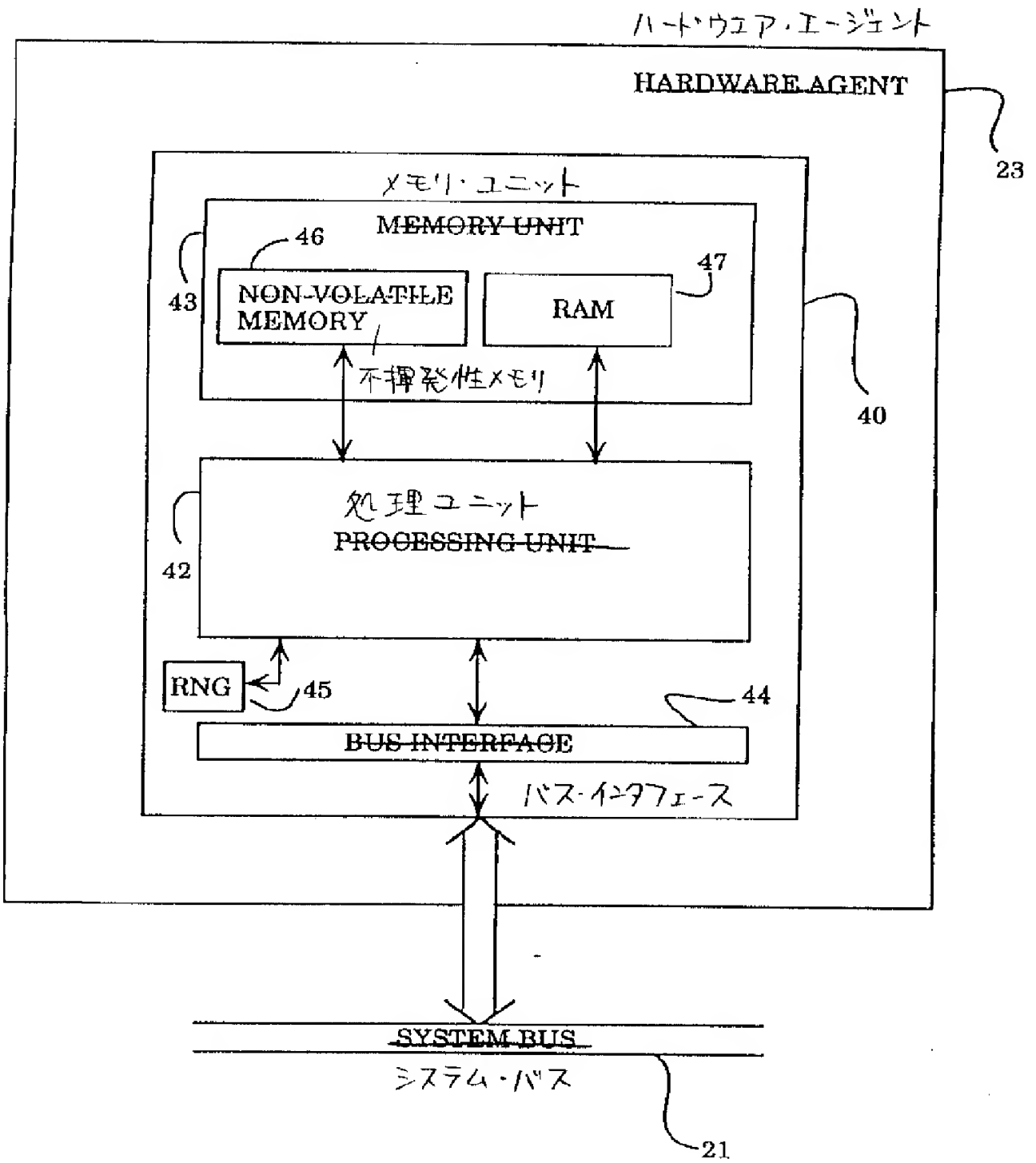

ハードウエア・エージェント
HARDWARE AGENT
23
メモリ・ユニット
MEMORY UNIT
46
47
43
NON-VOLATILE MEMORY
RAM
不揮発性メモリ
40
処理ユニット
PROCESSING UNIT
42
RNG
45
44
BUS INTERFACE
バス・インタフェース
SYSTEM BUS
システム・バス
21

Figure 5

【図６】

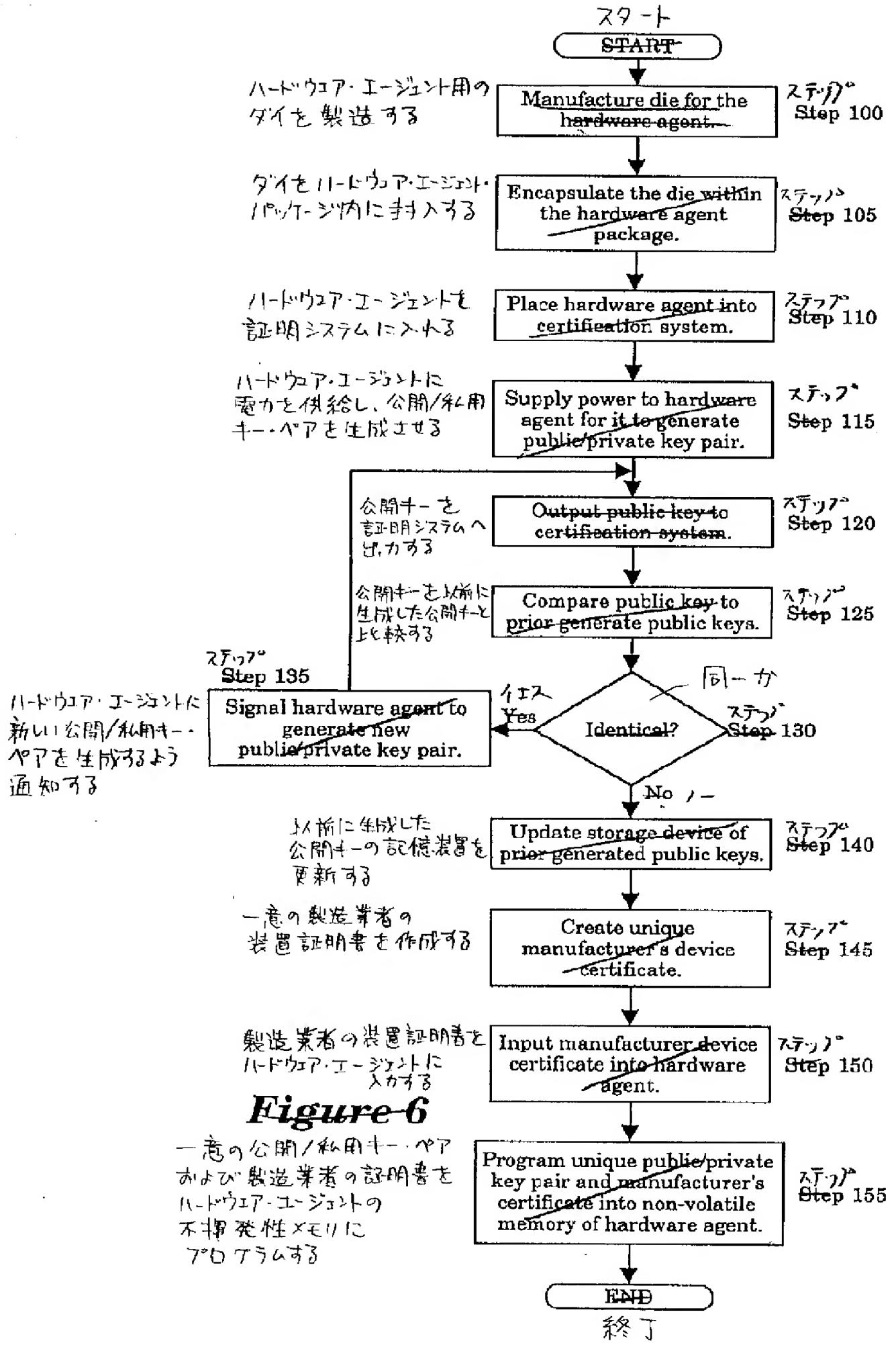

スタート
START
ハードウェア・エージェント用のダイを製造する
Manufacture die for the hardware agent.
ステップ Step 100
ダイをハードウェア・エージェント・パッケージ内に封入する
Encapsulate the die within the hardware agent package.
ステップ Step 105
ハードウェア・エージェントを証明システムに入れる
Place hardware agent into certification system.
ステップ Step 110
ハードウェア・エージェントに電力を供給し、公開/私用キー・ペアを生成させる
Supply power to hardware agent for it to generate public/private key pair.
ステップ Step 115
公開キーを証明システムへ出力する
Output public key to certification system.
ステップ Step 120
公開キーを以前に生成した公開キーと比較する
Compare public key to prior generate public keys.
ステップ Step 125
同一か
イエス Yes
Identical?
ステップ Step 130
ノー No
ステップ Step 135
ハードウェア・エージェントに新しい公開/私用キー・ペアを生成するよう通知する
Signal hardware agent to generate new public/private key pair.
以前に生成した公開キーの記憶装置を更新する
Update storage device of prior generated public keys.
ステップ Step 140
一意の製造業者の装置証明書を作成する
Create unique manufacturer's device certificate.
ステップ Step 145
製造業者の装置証明書をハードウェア・エージェントに入力する
Input manufacturer device certificate into hardware agent.
ステップ Step 150
一意の公開/私用キー・ペアおよび製造業者の証明書をハードウェア・エージェントの不揮発性メモリにプログラムする
Program unique public/private key pair and manufacturer's certificate into non-volatile memory of hardware agent.
ステップ Step 155
END
終了

Figure 6

【図７】

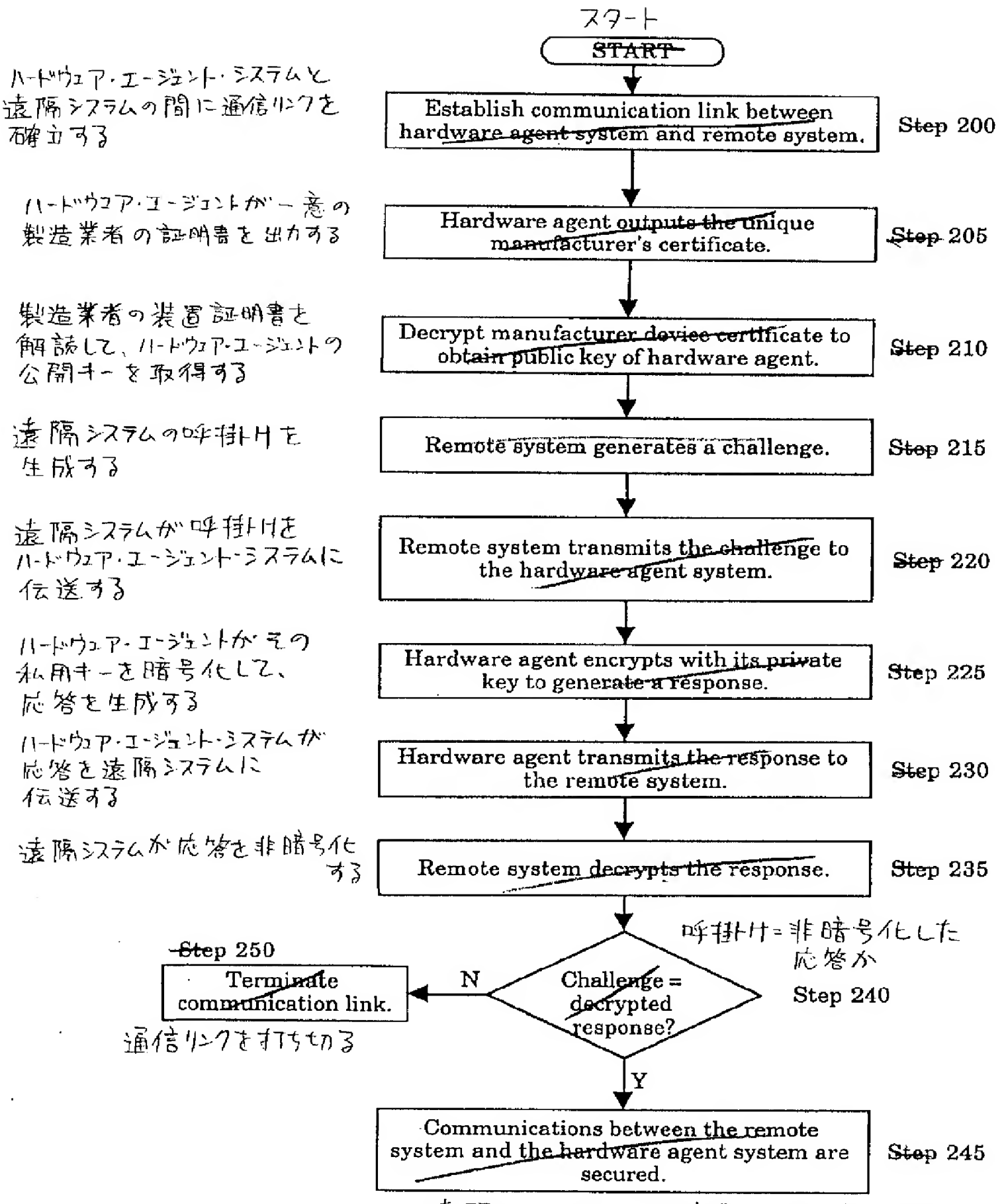

スタート
START
ハードウェア・エージェント・システムと遠隔システムの間に通信リンクを確立する
Establish communication link between hardware agent system and remote system.
Step 200
ハードウェア・エージェントが一意の製造業者の証明書を出力する
Hardware agent outputs the unique manufacturer's certificate.
Step 205
製造業者の装置証明書を解読して、ハードウェア・エージェントの公開キーを取得する
Decrypt manufacturer device certificate to obtain public key of hardware agent.
Step 210
遠隔システムの呼掛けを生成する
Remote system generates a challenge.
Step 215
遠隔システムが呼掛けをハードウェア・エージェント・システムに伝送する
Remote system transmits the challenge to the hardware agent system.
Step 220
ハードウェア・エージェントがその私用キーを暗号化して、応答を生成する
Hardware agent encrypts with its private key to generate a response.
Step 225
ハードウェア・エージェント・システムが応答を遠隔システムに伝送する
Hardware agent transmits the response to the remote system.
Step 230
遠隔システムが応答を非暗号化する
Remote system decrypts the response.
Step 235
呼掛け＝非暗号化した応答か
Challenge = decrypted response?
Step 240
N
Step 250
Terminate communication link.
通信リンクを打ち切る
Y
Communications between the remote system and the hardware agent system are secured.
Step 245
遠隔システムとハードウェア・エージェント・システムの間の通信は安全保護されている

Figure 7

【図８】

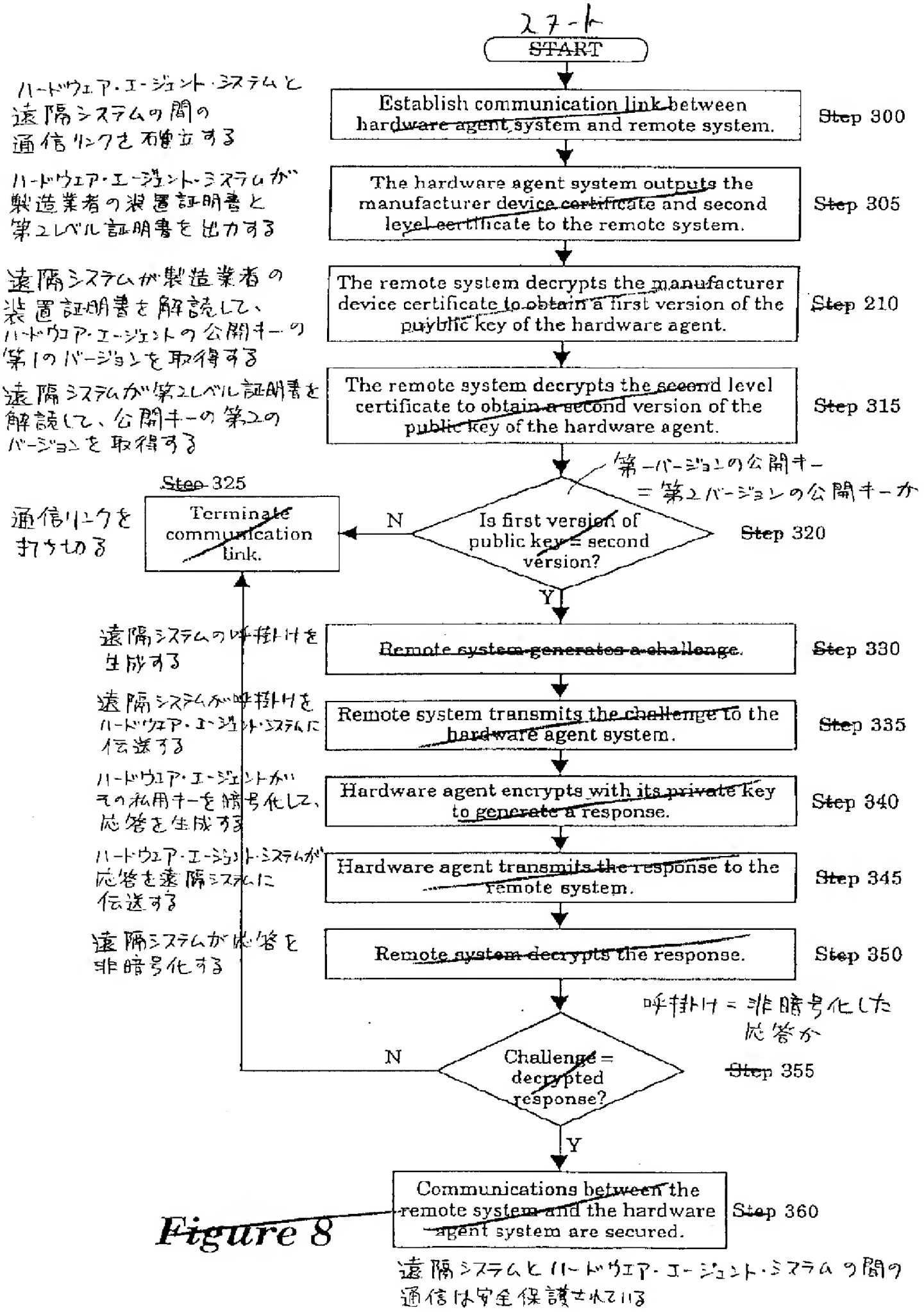

START
Establish communication link between hardware agent system and remote system.
Step 300
The hardware agent system outputs the manufacturer device certificate and second level certificate to the remote system.
Step 305
The remote system decrypts the manufacturer device certificate to obtain a first version of the public key of the hardware agent.
Step 210
The remote system decrypts the second level certificate to obtain a second version of the public key of the hardware agent.
Step 315
Is first version of public key = second version?
Step 320
N
Terminate communication link.
Step 325
Y
Remote system generates a challenge.
Step 330
Remote system transmits the challenge to the hardware agent system.
Step 335
Hardware agent encrypts with its private key to generate a response.
Step 340
Hardware agent transmits the response to the remote system.
Step 345
Remote system decrypts the response.
Step 350
Challenge = decrypted response?
Step 355
N
Y
Communications between the remote system and the hardware agent system are secured.
Step 360

Figure 8